# 802.1x と Web 認証 WLAN に関する LDAP 認証 を使用した WLC の設定

### 内容

概要 前提条件 要件 <u>使用するコンポーネント</u> 背景説明 技術背景 よく寄せられる質問(FAQ) 設定 LDAPサーバを使用して802.1x経由でユーザを認証するWLANの作成 ネットワーク図 内部WLC Webポータルを介してユーザを認証するLDAPサーバに依存するWLANの作成 ネットワーク図 LDAP ツールによる LDAP の設定とトラブルシューティング 確認 <u>トラブルシュート</u> 関連情報

### 概要

このドキュメントでは、LDAPサーバを使用してクライアントをユーザデータベースとして認証 するためにAireOS WLCを設定する手順について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Microsoft Windows Server
- Active Directory

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- Cisco WLC ソフトウェア 8.2.110.0
- Microsoft Windows Server 2012 R2

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく ださい。

### 背景説明

#### 技術背景

- LDAP は、ディレクトリ サーバへのアクセスに使用されるプロトコルです。
- ディレクトリ サーバは、オブジェクト指向の階層型データベースです。
- •オブジェクトは、組織単位(OU)、グループ、または既定のMicrosoftコンテナなどのコンテナ にCN=Usersとして編成されます。
- このセットアップで最も難しい部分は、WLC で LDAP サーバ パラメータを正しく設定する ことです。

これらの概念に関する詳細については、<u>『How to configure Wireless Lan Controller (WLC) for</u> Lightweight Directory Access Protocol (LDAP) authentication (Lightweight Directory Access Protocol (LDAP) 認証用のワイヤレス LAN コントローラ (WLC)の設定方法)』の「概要」の 項を参照してください。

### よく寄せられる質問(FAQ)

• LDAPサーバとのバインドに使用する必要があるユーザ名は何ですか。

LDAPサーバに対してバインドするには、匿名と認証済みの2つの方法があります(両方の方法の 違いを理解するには、を参照してください)。

このバインドのユーザ名には他のユーザ名とパスワードを問い合わせることができる管理者権限 が必要です。

•認証済みの場合:バインドユーザ名はすべてのユーザと同じコンテナ内にありますか。 いいえ:パス全体を使用します。以下に、いくつかの例を示します。

CN=Administrator,CN=Domain Admins,CN=Users,DC=labm,DC=cisco,DC=com

Yes:ユーザ名のみを使用します。以下に、いくつかの例を示します。

#### Administrator

・異なるコンテナにユーザが存在する場合はどうすればいいですか。関連するすべてのワイヤレス LDAP ユーザを同じコンテナに含める必要がありますか。

いいえ。必要なすべてのコンテナを含むベース DN を指定できます。

•WLCで検索する必要がある属性は何ですか。

WLCは、指定されたユーザ属性とオブジェクトタイプに一致します。

注:sAMAccountNameでは大文字と小文字が区別されますが、personでは区別されません

# 。したがって、sAMAccountName=RICARDOとsAMAccountName=ricardoは同じで機能しますが、samaccountname=RICARDOとsamaccountname=ricardoは機能しません。

• どのExtensible Authentication Protocol(EAP)方式を使用できますか。

EAP-FAST、PEAP-GTC、EAP-TLS のみです。Android、iOS、およびMacOSのデフォルトのサ プリカントは、Protected Extensible Authentication Protocol(PEAP)で動作します。

Windowsの場合は、図に示すように、Anyconnect Network Access Manager(NAM)または Cisco:PEAPを含むデフォルトのWindowsサプリカントを、サポートされているワイヤレスアダプ タで使用する必要があります。

Local-EAP Wireless Netw	ork Properties	x
Connection Security		
Security type: Encryption type:	WPA2-Enterprise	<b>•</b>
Choose a network aut	hentication method:	
Cisco: PEAP Microsoft: Smart Card Microsoft: Protected E Cisco: LEAP Cisco: EAP-FAST Intel: EAP-SIM Intel: EAP-SIM Intel: EAP-AKA Advanced settings	AP (PEAP)	Settings ion each work! works!
		OK Cancel

注:<u>Cisco EAP Plug-ins</u> for Windowsには、Cisco Bug ID <u>CSCva09670</u>の影響を受けるOpen Secure Socket Layer(OpenSSL 0.9.8k)のバージョンが含まれています。これ以降のリリー スではWindows用EAPプラグインを発行する予定はなく、代わりにAnyConnectセキュアモ ビリティクライアントを使用することをお勧めします。

・WLCがユーザを検出できないのはなぜですか。

グループ内のユーザは認証できません。図に示すように、デフォルトコンテナ(CN)または組織単位(OU)内に配置する必要があります。

	Name	Туре	Description
<u>.</u>	SofiaLabGroup	Group	will not work
-1	SofiaLabOU	Organizational Unit	
	Users	Container	Default container for upgr

## 設定

802.1x認証またはWeb認証のいずれかでLDAPサーバを使用できるさまざまなシナリオがあります。

この手順では、OU=SofiaLabOU内のユーザのみが認証されるようにする必要があります。

Label Distribution Protocol(LDP)ツールの使用方法、LDAPの設定およびトラブルシューティング については、『<u>WLC LDAPコンフィギュレーションガイド</u>』を参照してください。

### LDAPサーバを使用して802.1x経由でユーザを認証するWLANの作成

### ネットワーク図

このシナリオでは、WLAN LDAP-dot1xはLDAPサーバを使用して、802.1xを使用してユーザを認 証します。



### **LDAP Server**

à	Server Manager	_ 0 ×
€ Server M	lanager • Dashboard	- ②   🎢 Manage Took View Help
Dashboard	WELCOME TO SERVER MANAGER	Active Directory Administrative Center Active Directory Domains and Trusts Active Directory Lightweight Directory Services Setup Wizard
Local Server     All Servers     All CS	1 Configure this local server	Active Directory Module for Windows PowerShell Active Directory Sites and Services Active Directory Users and Computers
AD DS	2 Add roles and features	ADSI Edit Certification Authority Component Services
DNS     File and Storage Services ▷	3     Add other servers to manage       WHATS NEW     4       Create a server group	Computer Management Defragment and Optimize Drives DHCP
Ko IIS ¶∖ NAP		UNS Event Viewer Group Policy Management

#### Create User: SofiaLab User1 Test User

Account	Account			() × 🔊
Organization Member Of Password Settings Profile Policy Silo	First name: Middle initials: Last name: Full name: User UPN logon: Use SamAccountName o Password: Confirm password: Create in: DC alabm,DC aciss Find in this column	Sofialab User1 Test User Sofialab User1 Test User  Sofialab User1  Sofialab User1  Find in this column  Find in th	Account expires:	•
		Employees  ForeignSecurityPrincips  Guests  LostAndFound  =		) * • ) * •
	This object will be added	im Managed Service Accos + im NTDS Quotas + im Program Data + im System + v i to the default Active Directory group.		Add Remove

TASKS V SECTIONS V

#### Create User: SofiaLab User1 Test User

Create User:	SofiaLab User1	Test User				TASKS 🔻	SECTIONS 🔻	
Account	Account	Account						
Organization Member Of Password Settings Profile Policy Silo	First name:     SofiaLab User1     A       Middle initials:     Last name:     Test User       Full name:     * SofiaLab User1 Test User     Pa       User VBN Usgon:     Image: I				Never     End of		•	
	Organization			?ו				
	Member Of		Select Groups	×				
	Filter Name SofiaLabGroup	P Active Director Primary Isbm-SofiaLab	Select this object type: Groups or Built in security principals From this location: labin calco com Enter the object names to select (complete). Fortal abformed	Object Types Locations			Add Remove	
	This object will be added Directly Associated	I to the default Active Directory gro Password Settings Precedence	Advanced OK	Cancel			? 🖲 🔿	

### ステップ2:目的のEAP方式でWLCにEAPプロファイルを作成します(PEAPを使用)。

،، ،،، ،، cısco		MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>s</u> ecurit	Y M <u>A</u> NAGEMENT	Sa <u>v</u> e Configurati C <u>O</u> MMANDS	on   <u>P</u> ing HE <u>L</u> P	Logout   <u>R</u> efres <u>F</u> EEDBACK
Security	^	Local EA	P Profile	is				N	ew	Apply
▼ AAA General ▼ RADIUS		Profile Nar	me			EAP-FAST	EAP-TLS	PEAP		
Authentication Accounting Fallback DNS TACACS+		Local-EAP-L	EAP		✓					
LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies		LE EA EA	AP P-FAST P-TLS ΔP	Server   Server   Server   Server	Nothing PAK Certific	C   C cate   C	lient Userna lient Userna lient Certif	ame & Pass ame & Pass ficate ame & Pass	sword sword	
Ceneral General Profiles EAP-FAST Parameters Authentication Priority	,								, nor u	

ステップ 3:WLCをLDAPサーバにバインドします。

**ヒント**:バインドユーザ名がユーザベースDNにない場合は、次の図に示すように、 Adminユーザへのパス全体を書き込む必要があります。それ以外の場合は、Administratorと 入力します。

، المارينين ، ، ، ، ، ، ، ، ، ، ، ، ، ، ، ، ، ،	Sage Configuration Ping Logout Befn EDBACK
Security LDAP Servers > New	< Back Apply
✓ AAA       Server Index (Priority)       1 ♥       ■         General       Server IP Address       10.88.173.121         Authentication       Accounting       Port Number         Accounting       Port Number       39         Fallback       Bind Username       Authenticated ♥         LOAP       Bind Vsername       CN=Administrator, CN=Users, DC=labm, DC       Admin privile         Local Net Users       Bind Password       ●       ●         Jusabled Clients       User Base DN       OU=SofiaLabOU, DC=labm, DC=cisco, DC=com       Where         AP Policies       User Attribute       ■       ■       Whete         Password Policies       User Object Type       Person       ●       ●         I Local EAP       User Object Type       Person       ●	eges required re are we going to look for users? t Attribute are we looking for? ge from webpage Warning: LDAP can only be used with EAP-FAST, PEAP-GTC and EAP-TLS methods OK Cancel

ステップ4: [Authentication Order]を[Internal Users + LDAP or LDAP only]に設定します。

،، ،،، ،، cısco		MONITOR	<u>w</u> lans	CONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u>
Security	^	Priority C	)rder > L	ocal-Auth			
<ul> <li>▼ AAA</li> <li>General</li> <li>▼ RADIUS</li> <li>Authentication</li> </ul>		User Cred	lentials				
Accounting Fallback DNS TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies		Not Used	>	Order Used F	CAL	Up Down	]
<ul> <li>Local EAP</li> <li>General</li> <li>Profiles</li> <li>EAP-FAST Parameters</li> <li>Authentication Priority</li> </ul>						-	

### ステップ 5:LDAP-dot1x WLANを作成します。

uluili. cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	WLANs
WLANs	Current Filter: None [Change Filter] [Clear Filter] Create New V Go
Advanced	ULAN ID Type Profile Name WLAN SSID Admin Status Security Policies

ululu cisco	Monitor Wlans Controller Wireless Security Management Commands Help Feedback
WLANs	WLANs > Edit 'LDAP-dot1x'
WLANS	General Security QoS Policy-Mapping Advanced
▶ Advanced	Profile Name       LDAP-dot1x         Type       WLAN         SSID       LDAP-dot1x         Status       Image: Enabled         Security Policies       [WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
	Radio PolicyAllInterface/Interface Group(G)Vlan2562Multicast Vlan FeatureEnabledBroadcast SSIDImage: EnabledNAS-IDnone

手順 6:L2セキュリティ方式をWPA2+802.1xに設定し、L3セキュリティをnoneに設定します。

cisco	MONITOR	<u>W</u> LANs <u>C</u> ON	TROLLER \	WIRELESS	SECURITY	MANAGEN
WLANs	WLANs >	Edit 'LDA	P-dot1x'			
WLANs     WLANs	General	Security	QoS P	Policy-Mapp	oing Adv	vanced
Advanced	Layer 2	Layer 3	AAA Serv	vers		
	Layer	2 Security 🛍 🛛 MA	/PA+WPA2	~		
	Fast Trans	ition				
	Protected	l Management	Disable	d 🗸		
	WPA+WP	A2 Parameter	s			
	WPA P	olicy Policy		_		
	Authentic	Encryption	I AES	∐ ткір		
	802.1X CCKM	(	nable nable			
	PSK	<u></u> е	nable			
	FT 802	.1x	Enable Enable			
	WPA g	tk-randomize St	ate D	Disable 🗸		

手順 7:ローカルEAP認証を有効にし、[Authentication Servers]および[Accounting Servers]オプ ションが無効になっており、LDAPが有効になっていることを確認します。

،،ا،،،ا،، cısco	<u>M</u> ONITOR <u>W</u> LANs <u>C</u>	ontroller w <u>i</u> rel	ess <u>s</u> ecurity	M <u>a</u> nagement c <u>o</u> mn	1ANDS HE <u>L</u> P	<u>F</u> EEDBACK
WLANs	WLANs > Edit 'LI	DAP-dot1x'				
▼ WLANs WLANs	General Security	QoS Policy	-Mapping Adv	anced		
Advanced	Layer 2 Layer 3	3 AAA Servers				
	Select AAA servers b	elow to override use	of default servers o	on this WLAN		
	Radius Servers					
	Radius Server Over	write interface 🛛 En	abled			
	Authentication Serve	ers Accounting Serve	rs		EAP Paran	neters
		Enabled	En En	abled	Enable	
	Server 1	None	✓ None	~		
	Server 2	None	✓ None	$\checkmark$		
	Server 3	None	✓ None	$\sim$		
	Server 4	None	✓ None	~		
	Server 5	None	✓ None	~		
	Server 6	None	✓ None	~		
	Radius Server Accou	nting				
	Interim Update					
	LDAP Servers					
	Server 1 IP:10.8	8.173.121, Port:389 🗸				
	Server 2 None	~	]			
	Server 3 None	~	]			
	Local EAP Authentica	ition				
	Local EAP Authentic	ation 🗹 Enabled				
	EAP Profile Name	Local-EAP-PEA	AP 🗸			
	Authentication pr	iority order for we	b-auth user			
	Not Use	ed .		Order Used Fo	r Authentication	
			>	LOCA	L JS	Up
				JEDAP		

その他すべての設定は、デフォルトのままにすることができます。

注:

LDP ツールを使用して、設定パラメータを確認します。 [Search Base] をグループ(SofiaLabGroup など)にすることはできません。 Windowsマシンの場合は、サプリカントでMicrosoft:PEAPの代わりにPEAP-GTCまたは Cisco:PEAPを使用する必要があります。Microsoft:PEAPは、デフォルトで MacOS/iOS/Androidで動作します。

### 内部WLC Webポータルを介してユーザを認証するLDAPサーバに依存するWLANの 作成

ネットワーク図

このシナリオでは、WLAN LDAP-WebはLDAPサーバを使用して、内部WLC Webポータルでユー ザを認証します。

### LDAP Server



前の例のステップ1 ~ 4が完了していることを確認します。それから、異なる WLAN 設定を指定 します。

ステップ1:OU SofiaLabOUとグループSofiaLabGroupのLDAPサーバメンバーにユーザ**User1**を 作成します。

ステップ2:目的のEAP方式でWLCにEAPプロファイルを作成します(PEAPを使用)。

ステップ3:WLCをLDAPサーバにバインドします。

ステップ4: [Authentication Order]を[Internal Users + LDAP]に設定します。

ステップ 5:図に示すように、LDAP-Web WLANを作成します。

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	WLANs
WLANS	Current Filter: None [Change Filter] [Clear Filter] Create New V Go
Advanced	WLAN ID Type Profile Name WLAN SSID Admin Status Security Policies

iiliilii cisco	Monitor Wlans Controlle	er w <u>i</u> reless <u>s</u> ecurity	M <u>a</u> nagement (	C <u>o</u> mmands	HE <u>L</u> P	<u>F</u> EEDBACK
WLANs	WLANs > Edit 'LDAP-Web'					
WLANS	General Security Qos	Policy-Mapping Adv	anced			
Advanced	Profile Name Type SSID Status Security Policies Radio Policy Interface/Interface Group(G) Multicast Vlan Feature	LDAP-Web WLAN LDAP-Web Enabled [WPA2][Auth(802.1X)] (Modifications done under securit All Vlan2562 Enabled	y tab will appear aft	ter applying the	e change	s.)
	Broadcast SSID NAS-ID	✓ Enabled none				

手順 6:[L2 Security]を[none]に、[L3 Security]を[Web Policy - Authentication]に設定します。図に 示すように。

uluili. cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONTROLLER WIRELESS <u>S</u> ECURITY M <u>A</u> NAGEMENT C <u>O</u> MMANDS HELP <u>F</u> EEDBACK
WLANs	WLANs > Edit 'LDAP-Web'
<ul> <li>WLANs</li> <li>Mdvanced</li> </ul>	General       Security       QoS       Policy-Mapping       Advanced         Layer 2       Layer 3       AAA Servers         Layer 2       Security       None       T         MAC       Filtering?       T         Fast Transition       Fast Transition

،،ا،،،ا،، cısco	Monitor <u>w</u> lans <u>c</u> ontroller w <u>i</u> reless <u>s</u> ecurity m <u>a</u> nagement c <u>o</u> mmands he <u>l</u> p <u>f</u> eedback
WLANs	WLANs > Edit 'LDAP-Web'
WLANS	General Security QoS Policy-Mapping Advanced
Advanced	Layer 2 Layer 3 AAA Servers
	Layer 3 Security 1 Web Policy Authentication Authentication Conditional Web Redirect Splash Page Web Redirect On MAC Filter failure19 Preauthentication ACL IPv4 None IPv6 None WebAuth FlexAcl None Sleeping Client Enable Over-ride Global Config29 Enable Web Auth type Internal

手順 7: Web認証の認証の優先順位をLDAPを使用するように設定し、[Authentication Servers]および[Accounting Servers]オプションが無効になっていることを確認します。

cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONTROLLER W <u>I</u> RELESS <u>S</u> ECURITY M <u>A</u> NAGEMENT C <u>O</u> MMANDS HE <u>L</u> P <u>F</u> EEDBACK
WLANs	WLANs > Edit 'LDAP-Web'
WLANS	General Security QoS Policy-Mapping Advanced
Advanced	Layer 2 Layer 3 AAA Servers
	Select AAA servers below to override use of default servers on this WLAN
	RADIUS Servers
	RADIUS Server Overwrite interface Enabled
	Authentication Servers Accounting Servers
	Enabled Enabled
	Server 2 None Y None Y
	Server 3 None   None
	Server 4 None V None V
	Server 5 None V None V
	Server 6 None   None
	RADIUS Server Accounting
	Interim Update
	LDAP Servers
	Server 1 IP:10.88.173.121, Port:389 V
	Server 2 None
	Server 3 None T
	Local EAP Authentication
	Local EAP Authentication Enabled
	Authentication priority order for web-auth user
	Not Used Order Used For Authentication
	RADIUS A Vp
	✓ COCAL ✓ Down

その他すべての設定は、デフォルトのままにすることができます。

### LDAP ツールによる LDAP の設定とトラブルシューティング

ステップ1:LDAPサーバまたは接続されているホストのいずれかでLDPツールを開きます(サー バに対してポートTCP 389を許可する必要があります)。



ステップ 2: [Connection] > [Bind] に移動し、管理者ユーザでログインして、[Bind with credentials] オプションボタンを選択します。

Connectio	n Browse	View	0
Conn	ect		
Bind.		Ctrl+B	
Disco	nnect		
New		Ctrl+N	
Save			
Save	As		
Exit			

Bind ×						
User:	Administrator					
Password:	•••••					
Domain:						
Bind type Bind as currently logged on user Bind with credentials Simple bind Advanced (DIGEST)						
Encrypt traffic after bind     Advanced     Cancel     OK						

#### ステップ 3: [View] > [Tree] に移動し、ベースDNで[OK] を選択します。

12	_					ldap	)://V	VIN-4BD4NV0J3NK.labm.cisco.com/DC=labm,DC=cisco,DC=	com
Connection Brow	wse	View	Options	Utilities	Help			Tree Mary	x
	- 6	Tr	ree			Ctrl+T		Tree View	
	Enterprise Configuration     Status Bar								
					BaseDN:	<u> </u>			
		Se	et Font					Cancel OK	

ステップ 4:ツリーを展開して構造を表示し、検索ベースDNを探します。グループ以外のいずれ かのコンテナ タイプである可能性があることを考慮してください。ドメイン全体、特定の OU、 または CN=Users などの CN である可能性があります。



### ステップ 5:SofiaLabOUを展開して、その中に存在するユーザを確認します。前に作成した User1 が含まれています。

🙆 Idap://WIN-4BD4	NV0J3NK.labm.cisco.com/DC=labm,DC=cisco,DC=com	_	•	×
Connection Browse View Options Utilities Help				
■ DC=labm,DC=cisco,DC=com     CN=Builtin,DC=labm,DC=cisco,DC=com     OU=Computers,DC=labm,DC=cisco,DC=com     OU=Employees,DC=labm,DC=cisco,DC=com     OU=Employees,DC=labm,DC=cisco,DC=com     OU=Guests,DC=labm,DC=cisco,DC=com     ON=CN=Infrastructure,DC=labm,DC=cisco,DC=com     CN=LostAndFound,DC=labm,DC=cisco,DC=com     CN=NTDS Quotas,DC=labm,DC=cisco,DC=com     CN=Program Data,DC=labm,DC=cisco,DC=com     CN=SofiaLabGroup,DC=labm,DC=cisco,DC=com     CN=SofiaLabGU,DC=labm,DC=cisco,DC=com     CN=System,DC=labm,DC=cisco,DC=com     CN=System,DC=labm,DC=cisco,DC=com     CN=TPM Devices,DC=labm,DC=cisco,DC=com     CN=System,DC=labm,DC=cisco,DC=com     CN=Users,DC=labm,DC=cisco,DC=com     CN=Users,DC=labm,	Expanding base 'OU+SofiaLabOU,DC+labm,DC+cisco,DC+com' Getting 1 entries: Dr: OU+SofiaLabOU,DC-labm,DC-cisco,DC-com; distinguishedName: OU+SofiaLabOU,DC+labm,DC+cisco,DC+com; dSCorePropagationData (2): 8/10/2016 4:22:39 PM Central Daylight Time (Mexico); 0x0 = ( ); instanceType: 0x4 = (VRITE); name: SofiaLabOU; objectClase (2): top: organizationalUnit, CN+Schema,CN+Configuration,DC+labm,DC+cisco,DC+com; objectClase (2): top: organizationalUnit, objectClase (2): top: organizationalUnit, objectClase (2): top: organizationalUnit, ou: SofiaLabOU; uSNChanged: 45117; uSNChanged: 45116; whenChanged: 8/10/2016 4:22:39 PM Central Daylight Time (Mexico); whenChanged: 8/10/2016 4:22:39 PM Central Daylight Time (Mexico); whenChange: SofiaLab User1 Test User; cdstinguishedName: SofiaLab User1 Test User; displayName: SofiaLab User1 Test User; displayName: SofiaLab User1 Test User; displayName: SofiaLab User1 Test User; objectClass (4): top; Person; organizationalPerson; user; objectClass			
K III >				Y
Ready		NU	M	

ဂျကျက cisco	MONITOR WLANS CONTROLLER	WIRELESS SECURITY MANAGEMENT	Save Configuration Ping Logout Be COMMANDS HELP FEEDBACK
Security	LDAP Servers > New		< Back Apply
<ul> <li>AAA</li> <li>General</li> <li>RADIUS</li> <li>Authentication</li> <li>Accounting</li> <li>Falback</li> <li>DNS</li> <li>TACACS+</li> <li>LDAP</li> <li>Local Net Users</li> <li>MAC Fibring</li> <li>Disabled Clients</li> <li>User Login Policies</li> <li>AP Policies</li> <li>Policies</li> <li>Local EAP</li> <li>Priority Order</li> <li>Certificate</li> <li>Access Control</li> <li>Lists</li> <li>Wireless Protection</li> <li>Policies</li> <li>Web Auth</li> <li>TrustSec SXP</li> <li>Local Policies</li> <li>Advanced</li> </ul>	Server Index (Priority) Server IP Address Port Number Simple Bind Bind Username Bind Password Confirm Bind Password User Base DN User Attribute User Object Type Secure Mode(via TLS) Server Timeout Enable Server Status	1       ✓         10.88.173.121         389         Authenticated         CN=Administrator,CN=Users,DC=labm,DC=	Admin privileges required Where are we going to look for users? What Attribute are we looking for? Message from webpage Warning: LDAP can only be used with EAP-FAST, PEAP-GTC and EAP-TLS methods OK Cancel

手順 7:SofiaLabGroupなどのグループは検索DNとして使用できません。グループを展開し、そ のグループ内のユーザを探します。ここで、先に作成したUser1がを参照してください。

وَ الله عَنْ الله Activ	ve (	Directory Administ	rative Center • la	abm (local) 🔸		• 🗭   Manage Hel
Conversion	<	Iabm (Iocal) (16)       Filter       Name       Builtin       Computers       Domain Controllers       Employees       Foreign SecurityPrincipals       Guests       Infrastructure       LostAndFound       Managed Service Accounts       Program Data       SofiaLabGroup       SofiaLabCU       System       TPM Devices       Users	Image: Contract of Contract of Contract of Container         Organizational Unit         Organizational Unit         Organizational Unit         Organizational Unit         InfrastructureUpdate         IostAndFound         Container         msDS-QuotaContainer         Container         msDS-QuotaContainer         Container         msDS-QuotaContainer         Container         msDS-NuotaContainer         Container         msTPM-InformationObjectsC         Container	SofiaLabGro Group Managed By Member Of Members Password Settings Extensions	Oroup         Group name:       * SofaLabGroup         Group (SanAccountNam.*       SofaLabGroup         Group (SanAccountNam.*       SofaLabGroup         O Distribution       Global         Distribution       Global         Protect from accidental deletion         Managed By         Member Of         Image: Construction of the services Folder         SofaLab User1 Test User         Istim-SofaLabCU-SofaLab User1 Test User	Tasks
		E-mail: Managed by:		More Information	11	OK Cancel

User1 はありますが、それを LDP が見つけられませんでした。これは、WLCも同様に検索を実 行できないことを意味し、グループが検索ベースDNとしてサポートされていない理由です。

### 確認

ここでは、設定が正常に機能しているかどうかを確認します。

(cisco-controller) >show ldap summary

Idx Server Address Port Enabled Secure

--- ----- ------ ------

1 10.88.173.121 389 Yes No

#### (cisco-controller) > show ldap 1

Server Index	1
Address	10.88.173.121
Port	389
Server State	Enabled
User DN	OU=SofiaLabOU,DC=labm,DC=cisco,DC=com
User Attribute	sAMAccountName
User Type	Person
Retransmit Timeout	2 seconds
Secure (via TLS)	Disabled
Bind Method	Authenticated
Bind Username	CN=Administrator,CN=Domain
Admins,CN=Users,DC=labm,DC=cisco,DC=com	

# トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

(cisco-controller) >debug client <mac address=""></mac>	
(cisco-controller) >debug aaa ldap enable	
(cisco-controller) >show ldap statistics	
Server Index Server statistics:	1
Initialized OK 0	
Initialization failed 0	
Initialization retries 0	
Closed OK 0	
Request statistics:	
Received	
Sent0	
ок0	
Success	
Authentication failed0	
Server not found0	
No received attributes	
No passed username	
Not connected to server	
Internal error 0	
Kerites A	

# 関連情報

- <u>『LDAP WLC 8.2 Configuration Guide(LDAP WLC 8.2 設定ガイド)』</u>
- <u>『How to configure Wireless Lan Controller (WLC) for Lightweight Directory Access Protocol (LDAP) authentication (Lightweight Directory Access Protocol (LDAP) 認証用のワイヤレス LAN コントローラ (WLC)の設定方法)』(著者: Vinay Sharma)</u>
- Web Authentication Using LDAP on Wireless LAN Controllers (WLCs) Configuration
   Example (ワイヤレス LAN コントローラ (WLC) での LDAP による Web 認証の設定例) (著者: Yahya Jaber および Ayman Alfares)
- <u>テクニカル サポートとドキュメント Cisco Systems</u>

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。